Privacy and Security Tiger Team
Draft Transcript
March 7, 2011

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good morning, everybody, and welcome to the Privacy and Security Tiger Team. This is a Federal Advisory Committee, so there will be opportunity at the end of the call for the public to make comment. Workgroup members, please remember to identify yourselves when speaking.

Let me do the roll call. Deven McGraw?

Deven McGraw – Center for Democracy & Technology – Director
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Paul Egerman?

Paul Egerman – Software Entrepreneur
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Latanya Sweeney? Gayle Harrell? Carol Diamond?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Judy Faulkner? Carl, are you on?

Carl Dvorak – Epic Systems – EVP
Carl Dvorak's here on behalf of Judy.

Judy Sparrow – Office of the National Coordinator – Executive Director
David McCallie? Neil Calman couldn't make it today. David Lansky? Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Micky Tripathi? Rachel Block? Alice Brown?

Alice Brown – National Partnership for Women & Families – Director HITP
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
John Houston?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director

Wes Rishel? Leslie Francis?

Leslie Francis – NCVHS – Co-Chair
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Adam Greene?

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Lisa Tutterow? Joy Pritts?

Joy Pritts – ONC – Chief Privacy Officer
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Did I leave anyone off?

Lisa Tutterow – Office of the National Coordinator – popHealth Principal
Lisa Tutterow is here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay, thank you. I'll turn it over to Deven.

Deven McGraw – Center for Democracy & Technology – Director
Great, and I'm going to turn it over to Paul.

Paul Egerman – Software Entrepreneur
I'm going to say good morning and welcome to our tiger team meeting on this bright and warm and sunny Monday morning. We're very happy to have everybody participating in this call. To remind everybody, the Privacy and Security Tiger Team is a group that was formed from members of the Policy Committee and the Standards Committee to address a number of privacy and security topics. The topics that we are working with right now relate to authentication. Today's topics really relate to EHR user authentication and the beginning of a discussion about identity proofing and authentication for patients. So the topic is really authentication, but it really starts with the EHR users and then, depending on our time frame, hopefully proceeds to a discussion about identity proofing and then authentication for patients.

To describe the scope of today's discussion we will be discussing feedback from the HIT Policy Committee. Deven and I made a presentation, I guess it was last week, to the Policy Committee on the work that this tiger team has done so far on user authentication, and we got some excellent feedback that we want to review with you. The second topic, as I said, is to begin our discussion on patient access to EHRs. The comment we also want to make is that if you look at the schedule, we have two meetings in March, so just today's meeting and also on March 23rd. Our goal is to try to complete our recommendations on authentication in this time frame and so that we can review as a group the recommendations on March 23rd and then submit them to the Policy Committee for its April meeting on April 13th. That's the goal. The goal is to complete the discussions during the month of March.

The first topic again is the EHR user authentication. We list here some assumptions, but I first want to briefly remind everybody what an EHR user is. An EHR user is a physician or other healthcare professional or clinician, or an administrative person or an executive, who accesses the EHR system. In some sense, it's everybody except patients. If this was any other industry you might call these people employees, but that doesn't work quite in healthcare. In some of our slides, we call them staff, but actually, it doesn't quite work either. But I think we know what an EHR user is, and the assumptions are that this user has already received their credentials, in other words, whatever passwords or other

materials that they need they've already received. The assumption also is that the entity is already following the HIPAA security rule, and that means they've put in place the appropriate administrative, technical, and physical safeguards so that those are like our foundation assumptions.

Also, there are these other two comments here. It's important to remember, we're talking about authentication, but that's only one component of the entire security process. There's also something else called authorization, which basically says that after you've been authenticated what you're allowed to do. So that's also part of the process and there are other critical measures, including audit trails, that monitor the appropriateness of access and encryption. That's all the basic assumptions as to where we have been so far.

The previous tiger team discussions that we've had, this tiger team felt that remote access raised heightened security risks. What is remote access? Remote access is access over a public network, probably the Internet, and that is probably access that could occur at home or it could possibly occur through a handheld device. The tiger team did look to NIST assurance levels, and basically in our previous discussions we felt that Level 3 assurance made sense in the context of remote access, and there's this comment on the bottom of your slide here that's very important. It says, "Achieving Level 3 means that there is a high degree of confidence that a claimant in an authentication process is actually who they claim to be."

So where we've been so far is we sort of felt like Level 3 made sense, we got that far, and as part of that we felt that more than just log-in and password should be required. In other words, we felt that it should be more than one factor, such as two factor or multi factor. Those are things that were also consistent with Level 3. But in our last discussion we did not have a consensus yet on that Level 3 or anything else with a specific baseline requirement regarding factors, so we're comfortable with Level 3 or comfortable with more than one factor, but we didn't really say yes, that's what we want to do. The reason we didn't was this last comment too, is we were also concerned about how do you balance utility with risk. So there was some concern, well, gee, can we set Level 3 as a one size fits all? That's the best summary that I can do of where we've been so far. Let me pause to see if people want to add anything, if you feel that summary is accurate.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Paul, for my edification can you define what would be multi factor or two factor?

Paul Egerman – Software Entrepreneur
Well, great question. Basically, the factors go into three categories. It's what you know, what you have, and something unique about you. So a two factor authentication process would be, password would be one factor potentially. The second factor could be something that you possess, so it could be a card with a magnetic stripe. It could be a card that has one of these numeric numbering sequences that change over time. That could be a second factor. Somewhat arguably, biometrics could be a second factor. So that would be two factors consistent with the way we've been discussing it so far. There has been some discussion as to whether or not the second factor could be also something you know, which is not consistent with NIST Level 3, but that would also—

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Let me ask you a question. The reason why I bring it up is that, my organization got away from using the little card that has a number that changes towards sort of a banking type of second factor, which is a downloadable applet to a computer. Part of the reason why I bring this up is the concern out of the physician community about if I have tokens from all these different providers and I have to have this token or that token how do I manage all of this? So I was just wondering how slim a second factor it could be.

Paul Egerman – Software Entrepreneur
That question is exactly the question we ended our discussions with. As I describe factors, you mentioned something on the computer. There's a digital certificate on the computer that is a second factor or a second token. The issue is, what is the right way to do more than one token? Was somebody trying to say something?

Carl Dvorak – Epic Systems – EVP
Paul, I think we want to be really careful when referencing the missed levels because I think this Level 3 is a bit more strict than we're discussing right now. I think in this Level 3 would require a biometric check, like a fingerprint, voice scan, palm scan, iris scan type of thing, or a revocable token like the little key fob that spits out a unique number. I think the revocability of a token app or coming from a specific identified IP address was an important element in differentiating this Level 3 from a swipe card that might just have our user ID on it from which we enter our password. I think there's an element of a deeper revocability in this Level 3, if I recall correctly. So we may want to research that at more depth, because I think there are some subtleties as you go from two to three.

Paul Egerman – Software Entrepreneur
Carl, you're exactly right. When we got to Level 3, I tried to describe on the slides. On the one hand, if you look at the issue strictly from a security standpoint you can be very comfortable at Level 3 and it is a fairly stringent security level. But the issue, as it says on the last sentence of the slide, is well how do you balance utility and risk?

Carl Dvorak – Epic Systems – EVP
I absolutely—

Paul Egerman – Software Entrepreneur
So that's the fundamental issue. When you talk about it from a security standpoint, I think you get pretty comfortable pretty fast with Level 3 but then when you start to look at issues that you just raised and the issue that John just raised in terms of what he's talking about. Then you're talking about taking a little bit of a step back from Level 3.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
One thing that Carl said was not accurate, in that this document excludes, remember at our last discussion, it excludes the use of biometric as a second factor. It doesn't require it. It doesn't even allow it.

Paul Egerman – Software Entrepreneur
That's correct.

Carl Dvorak – Epic Systems – EVP
Oh, really? Okay.

Deven McGraw – Center for Democracy & Technology – Director
Yes, I think in the backup slides, if it's not in this stack, it was definitely in a previous one. They specify with a little bit more detail how NIST SP 800-63 treats biometrics. But again, it differs. It differs from where DEA landed. We thought from a conceptual standpoint we wanted a high degree of confidence in the authentication process, which lands you on three from an assurance level, but then when you get to what types of authentication are required, either under NIST or other frameworks to get there, that's where we broke down.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The other point I think that would be useful in level setting here is to point out a discussion at our last meeting about the fact that the ePrescribing for controlled substances uses Level 3 but does allow biometrics. So that's a point that we've been discussing.

Paul Egerman – Software Entrepreneur
That's right. So the Level 3 does not include biometrics, although what we call the DEA approach, that's probably not the right terminology, the DEA approach for ePrescribing for controlled substances does permit biometrics. So one of the ideas on the table was use that as the baseline for everything, because at least there would be some consistency, but the purpose of my little spiel here is that I was trying to make sure we tried to get ourselves back to the same level that we were at in our previous discussion.

Then again, to summarize this we got to the idea of a Level 3, we got the idea that Dixie just said, which was that the rules for controlled substance ePrescribing is a Level 3 plus biometrics so that that helps a little bit. But once we got to that point exactly as promises came from Carl and John, we looked at this issue of utility and risk and people said, do we want to set a base level at this point, or do we want to back off it a little bit? That's where we were. I don't think we came to any conclusions. I think that's where we were.

Deven McGraw – Center for Democracy & Technology – Director
We didn't. But what we did do was we were able to tee up that discussion for the Policy Committee.

Paul Egerman – Software Entrepreneur
Right, and I think Deven's going to take us through that in a minute. First, let me make sure that we're at a baseline. First, I don't know if people who were on the previous call feel that I described it accurately. Does anybody have anything they want to add? Does anybody have any questions about what I said so far?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Paul, I don't have anything to add. I think you summarized it well, but I just want to let you know I joined the call a little bit late.

Paul Egerman – Software Entrepreneur
Thank you, David. I'm glad to have you.

Joy Pritts – ONC – Chief Privacy Officer
I'm here too.

Deven McGraw – Center for Democracy & Technology – Director
Hi, Joy.

Paul Egerman – Software Entrepreneur
Hi, Joy. It's good to see you. It's good to hear from you, actually. I cannot see you. That would be, I guess, a different level of biometrics.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Joy Pritts – ONC – Chief Privacy Officer
I think it's called a hologram maybe.

Paul Egerman – Software Entrepreneur
Right.

Deven McGraw – Center for Democracy & Technology – Director
Your avatar.

Paul Egerman – Software Entrepreneur
But not having any comments, why don't we proceed then, Deven, on the next slide. I think you're going to give us feedback on the Policy Committee. So we presented this material to the Policy Committee, and Deven will tell you what it is.

Deven McGraw – Center for Democracy & Technology – Director
I'm going to take us through some points on the slide. But I know there were others who were present at the meeting and we just want to capture the comments. I really think in general we got a very similar set of feedback in terms of the issues we were struggling with, and they were quite similar to the same issues that we had teed up ourselves. And that is, overall we understand that the public must trust these systems. So therefore that leads you to want to achieve Level 3 through the recommended processes

with multi factor authentication of some type, but at the same time it needs to be usable by providers, and again that same sort of balance of utility and risk concerns were raised by the committee themselves.

Others talked about how there are some other initiatives going on in the federal government, which includes this National Strategy for Trusted Identity in Cyberspace, which could be quite relevant here. But that strategy, which was issued in very preliminary draft form several months ago is, number one, not done, and the early draft actually didn't have some very clear direction set in terms of whether there would be levels of authentication that would be sought to achieve and what would be the factors, etc. Some suggested that once providers adjusted to requiring at least two factors most could adapt to it fine, particularly if they were able to use those same credentials across multiple organizations, which gets to the point that John raised about how it's not easy when you have a hard token for every single facility where you have privileges, for example. Then Dr. Blumenthal actually raised the notion that stronger authentication requirements could be a deterrent to the theft of physician identity, which is a recurring problem that contributes to Medicare fraud and other types of financial fraud.

The other thing we heard, I think pretty clearly, was that Dr. Blumenthal himself was strongly supportive of at least two factors, and suggested that maybe where we ought to focus our recommendations is on what's required to participate in the National Health Information Network, versus necessarily having the scope of our requirements addressing how entities handle access to their own EHRs. Again, to continue to allow them to do what they think is necessary to meet with their security rule obligations but to set a higher standard for the National Health Information Network.

So I want to pause there and ask Paul first if he thinks we captured here the right comments that came in from the Policy Committee, and then open it up to others who are on the line who want to comment on this.

Paul Egerman – Software Entrepreneur
Yes, Deven, I think you did a great job of describing it. I have to say one of the things that surprised me a little bit was to see the physicians on the Policy Committee seeming to be the ones that were pushing hardest for security. Dr. Blumenthal, Dr. Tang, and Dr. Calman all seemed to be saying go for it. I was a bit surprised. I don't know if that's because they're physician executives and that's what they're used to doing is implementing things, but somehow I would have suspected that they would have been more sensitive to some of these utility issues. That's what I heard. The CIO present, Marc Probst from Intermountain, basically advocated for slightly less than this Level 3, although he explained that Intermountain does do two factor and Level 3 for all of its remote use. So it was an interesting discussion.

Deven McGraw – Center for Democracy & Technology – Director
Does anybody else from the tiger team who was present for the Policy Committee discussion want to add anything in terms of any feedback that we missed from the committee, given the feedback that we got, particularly from Dr. Blumenthal—and we'll get, in a second—to the set of straw recommendations that we developed to kick off our discussion on where do we go from here?

Carl Dvorak – Epic Systems – EVP
I was listening in on the meeting through the computer, and one thing I noticed that was said, I think by David himself, was with regard to access of the NHIN or NW-HIN, whatever the name of it is currently, that in that case the stronger authentication would be required. Yet one of the things I realized was that much of the access to the Nationwide Health Information Exchange will actually take place without the doctor being logged in, either in preparation for their visit or subsequent to an encounter. Maybe before you transmit the thing, you're going to want the lab tests back, so the doctor may in fact not be logged in and yet you'll want to complete those transactions with the health information exchanges and with the Nationwide Health Information Exchange. So I think there's a presumption of synchronicity between a physician being logged on and a transaction taking place that I just don't believe will actually be there in a very significant percentage, if not the majority of cases, that we actually experience in real life.

Deven McGraw – Center for Democracy & Technology – Director

We do have the recommendations that we've done on entity authentication, so in terms of delivery of results to the appropriate entity level EHR, did we not have a set of recommendations that took care of that in terms of issuance of digital certificates?

Carl Dvorak – Epic Systems – EVP
I thought we were on the right path before. I guess I raised this concern just to make sure we don't accidentally overrule that other path, which I think was correct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I agree with Deven that that's an entity level that we've already discussed.

Carl Dvorak – Epic Systems – EVP
I agree as well. I just want to make sure that this new ... didn't overrule that.

Deven McGraw – Center for Democracy & Technology – Director
Yes, we need to keep that in mind.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I do have a question—

Paul Egerman – Software Entrepreneur
I'm sorry, Dixie, were you saying something?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I want to make sure I wasn't talking over someone. I had a question about when you spoke with the Policy Committee, I'm sorry I wasn't able to listen in on that, but did the topic of need for synchronicity with the DEA rule come up at all?

Deven McGraw – Center for Democracy & Technology – Director
We teed that up as one of the possibilities that we had discussed. I think folks recognize that that rule was out there and would apply to certain transactions, but the same set of concerns about wanting strong authentication but also wanting to make sure we would maximize utility for the providers, not overburden them, and have a system that worked also came up. I don't recall that anybody specifically said, yes, let's do DEA because it's already required in some circumstances, versus no, let's not do DEA. I think the conversation continued to circle around the larger picture issues of do you require at least two factor authentication of some sort or another, whether it's the strict NIST 800-63 approach or whether it's the DEA approach or do you compromise on that a bit, and that was where the conversation circled. Did I miss something? It didn't center around do DEA or don't do DEA.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I really was referring to the fact that DEA differs from NIST in that it allows biometrics.

Deven McGraw – Center for Democracy & Technology – Director
We had a little bit of a discussion about whether that was a critical distinction and some discussion about the value of biometrics that I think in essence concluded that it was not really our task to dive deeply into the efficacy of biometrics authentication methodologies, and that instead we were better sticking to the larger policy questions.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I thought that was a policy question, whether we needed to be consistent with what DEA is requiring.

Deven McGraw – Center for Democracy & Technology – Director
But the policy question of consistency with DEA not drilled down to the level of is biometric a factor or not, but at the level of do you require two factors.

Paul Egerman – Software Entrepreneur

Dixie, what happened is during the Policy Committee meeting the distinction between Level 3 and the DEA approach, that was not a major concept of that discussion. It was there on the slides, but the discussion was a little bit more general, which was how strict do we want to be. It was a little less specific. It was more general. How strict are we going to be? The feedback was on the side of being strict. I don't know if "strict" is the right word for a security person, but that's my interpretation.

I want to also get back to Carl's comment. Carl made an excellent comment that there's an image that some people might have that the way the NHIN or NW-HIN works is physicians are themselves signing on to other computer systems or HIEs and directly accessing the information across organizational boundaries. As Carl is pointing out, there's a massive amount possibly, or probably the majority of the amount doesn't work that way, where information flows back and forth with laboratory results, and certainly ePrescribing is also—well ePrescribing does involve physicians, but there's a lot of examples where the information simply flows back and forth. But the comment that was made, and it's an important comment, was that there was an analogy of NHIN to the air traffic controller system. The comment was the way the air traffic controller system works is security is only as good as like the weakest link, the weakest airport. The concept is if we go to a true nationwide health information network, similarly, especially when you talk about remote access, the security of the entire nationwide system might only be as good as the weakest link. If there is some group that has the ability to sign on to their system that is not protected, and sign on remotely and then they're connected to the NHIN, then the fear is that's an on ramp for somebody to gain access to information. I'm not trying to advocate for that position, as much as to say I think that was part of the understanding that people had.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Paul, just a few other things that I heard at the meeting and want to raise. I know David Lansky talked about the lack of evidence for different approaches and that that's—

Paul Egerman – Software Entrepreneur
Yes.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
—... really don't have much knowledge as to what works and what works better. I know Larry, with respect to DEA, talked about that it would be useful to get more field experience on how the DEA standard actually works in practice. Then Marc from Intermountain, and I know this has been the minority approach, talked about technology providing potentially alternative methods of keeping data safe and the importance of providing flexibility to support innovation. I just wanted to add those two.

Deven McGraw – Center for Democracy & Technology – Director
Thank you, Adam, those absolutely were points that were made. Again, underscoring that while there was certainly some support for declaring Level 3 with some version of multi factor authentication, those points were very strongly made. I really don't think that if we had asked the committee to take a vote on a specific recommendation that we could necessarily have achieved consensus at the place where we were last—

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Deven, I was just going to say, could part of our recommendation be that research be done? In other words, this issue of really not having the data to support different modalities, particularly what's considered the gold standard in person proofing, this was a big surprise to us in our work in Connecting for Health when we worked on this issue. Even though in person proofing has become the gold standard, we just couldn't find any data on how well it worked. I wonder if part of our recommendation couldn't be that some research funding be dedicated to evaluating each of these methodologies and potentially evaluating them in different settings.

Deven McGraw – Center for Democracy & Technology – Director
I think that's a great idea, Carol. I'm trying to remember if we included that in some of the recommendations or not. If not, we should definitely add that to the list.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes, they're definitely in our recommendations, in the Connecting for Health regulations, but I don't know if they're in the tiger team recommendations.

Deven McGraw – Center for Democracy & Technology – Director
Exactly. I'm trying to remember if we pulled that into the draft slides, and we'll find out in a second. It's a very good point. Why don't we go ahead and take a look at that based on that feedback, and thanks to all who augmented it. It was quite the discussion, as is almost always the case with anything we bring before the Policy Committee. So what we did was to come up with a set of recommendations that really do key off from Dr. Blumenthal's suggestion that we look to creating some criteria for the Nationwide Health Information Network, which I've abbreviated here using the old abbreviation. I'll acknowledge that that's either unsettled or I've gotten it wrong, but these recommendations are intended to mean the Nationwide Health Information Network. I just want to go through these quickly to frame the whole picture, and then we'll go back and talk about them.

We have a requirement with respect to participation in the Nationwide Health Information Network, which is at least at an assurance level we want authentication at NIST Level 3. Consequently, you need two factor authentication for access to identifiable health information via the Nationwide Health Information Network. Then there are some options there. Do you go with NIST Level 3, which has an impact on the use of biometrics? Do we suggest DEA? Do we say any two factors? Or, do we not weigh in on the specific two factors, or maybe even ask the Standards Committee to specify the factors for demonstrating two factor authentication? And we can even couple that with a recommendation that the two factors be from different categories, which is consistent with a NIST approach. Then, ONC should be helpful in explaining to providers what the benefits are of these additional protections. Whatever the policies are for the Nationwide Health Information should be reassessed for consistency with other national identity efforts and technology developments.

Then in terms of what outside of what's required to participate in the NHIN with respect to access to an organization's own EHR, rather than specifying necessarily that that should be Level 3 with at least two factors, we should instead suggest that the Office of Civil Rights, which we don't directly provide recommendations to. So these would be more bully pulpit style, OCR could consider updating the HIPAA security rule and/or providing guidance to reflect greater concerns with respect to remote access by employees, staff, and internal personnel to an entity's EHR.

So the difference in these straw man recommendations from ones that we had on the table before is that—and I'm just going to go back to the beginning—we are drawing a distinction between what's required to be using the Nationwide Health Information Network brand. To say that you are a participant in Nationwide Health Information Network you need to follow two factor authentication for access to identifiable information. With respect to what an organization does in terms of access to its own EHR, which is really governed by the security rule, we're not suggesting that our recommendation apply to that, but we are encouraging the Office of Civil Rights to reassess remote access in particular and what that means for security rule compliance. I see now that we did not add Carol's point about promoting greater research into the efficacy of various authentication combinations and settings, but I certainly would be supportive of adding that. It was a good point and it's one that was definitely teed up by the Policy Committee discussion. I want to stop there.

Paul Egerman – Software Entrepreneur
Deven, when we say "requirement" we're saying requirement for remote access.

Deven McGraw – Center for Democracy & Technology – Director
What do you mean?

Paul Egerman – Software Entrepreneur
In other words, the authentication must be Level 3 two factor authentication, we're requiring that for remote access to the EHR, as opposed to within the enterprise.

Deven McGraw – Center for Democracy & Technology – Director
Are you talking about for participation in the Nationwide Health Information Network or what we're suggesting—?

Paul Egerman – Software Entrepreneur
Yes, what our proposed recommendation is.

Deven McGraw – Center for Democracy & Technology – Director
Okay. I think it's a good question, Paul. I'm not sure that the recommendation is terribly specific on that. Instead, what I think we were intending to propose was to follow Dr. Blumenthal's lead to say that we can and should create a higher trust level for an individual provider to authenticate to an NHIN, or the NW-HIN, or whatever we're calling it. Again, keeping in mind that we already have the certificate requirements for entity participation, which one would hope would be part of the Nationwide Health Information governance rules. This would be about individual authentication with respect to access of information through the Nationwide Health Information Network, and then I think it's a discussable question about whether that recommendation itself would be limited to remote access only. Because the intent with these straw recommendations was to draw a bit of a distinction between what higher level requirements might be for authentication at an individual level for access through the Nationwide Health Information Network, versus what entities themselves should do internally with respect to access to their own EHRs, whether that's on site or remote.

Carl Dvorak – Epic Systems – EVP
Deven, you're suggesting that we would write something up to clarify that if an organization had appropriate certificate for the NW-HIN, that a physician who was inside the network at that organization, although not using a Level 3 authentication approach, would not need to do anything further. So if there were a Level 2 inside the wire but their organization subsequently sent the transaction on behalf of that physician over the NW-HIN, then we would clearly call that case out, that's what you're suggesting, as being an approved case?

Deven McGraw – Center for Democracy & Technology – Director
Well, because it says "through the entity," and so don't we depend on – I think it's worth discussing, Carl. So I don't know that I can even answer your question, because that to me sounds like if it's sent by the entity through the EHR then that would be taken care of by the entity certificate under recommendations that we've already made.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think that the EHR to NW-HIN security would be fine. The question is who's sitting in front of the EHR. I think it's going to be really tricky to define this notion of internal or external. If a physician from home establishes a VPN session to his hospital's EHR and then turns and accesses the NHIN, is that inside or outside? I don't think there's any technical way you can tell.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
To that point, you're saying at that point when the physician decides to remotely access information via his EHR to the NHIN, that that would invoke these recommendations whereby there had to be two factor authentication?

Deven McGraw – Center for Democracy & Technology – Director
In other words, I think what I had intended here is not that narrow of a use case, John. I think what I intended was to say that the entire trust level that we are seeking for health information exchange, we ought to impose as a condition of participation in the Nationwide Health Information Network versus focusing our policy recommendations necessarily on changes in the HIPAA security rules.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I'm being very dense.

Deven McGraw – Center for Democracy & Technology – Director

I'm probably being denser, John, so you're fine with the question. I want people to understand at a higher level what I'm trying to do here, and that is to say that we potentially have a vehicle. Almost one could argue an invitation from the national coordinator to use this vehicle to impose a higher level of expectation for authentication for participants in the Nationwide Health Information Network versus doing what essentially the DEA did and imposing a higher authentication requirement as a de facto baseline standard that would apply across the board. And there might be two reasons to do this. One is, I think there's a general acceptability among Policy Committee members that creating higher expectations for Nationwide Health Information Network participation is an acceptable policy vehicle. It's also within the authority of ONC to establish or impose or have oversight over, versus thinking of the universe as essentially all potential exchangers, whether they're choosing to be part of the Nationwide Health Information Network or not.

Then we're straying into oversight mechanisms that we don't necessarily directly advise, that the Office of the National Coordinator isn't necessarily in control over. And particularly given the uncertainty that people feel in terms of not really having a good evidence base about which types of authentication necessarily work better than others, that maybe doesn't justify a more sweeping recommendation that would attach to all providers. So that's what I'm struggling with, is trying to take the opportunity and suggestion that was given to us at the Policy Committee that we look to criteria for participating in the Nationwide Health Information Network and then define what that looks like. Whether that's even internal access to one's own system remotely or whether there's some other types of individual access involved in the Nationwide Health Information Network that we would want to define and scope out.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Deven, let me restate what I think you just said. It actually made sense to me all of a sudden, so maybe I heard you correctly finally.

Deven McGraw – Center for Democracy & Technology – Director
Maybe you're going to restate it in a way that it will make sense to everybody, and I'll be eternally grateful to you.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Well, I'm not sure. You can make the analogy that ePrescribing of controlled substances is such a sensitive area that even though for ordinary ePrescribing you don't have to meet the level of assurance that the DEA has defined, if you write a prescription for a controlled substance you do have to prove a certain level of identify assurance. The same analogy could be made with respect to the EMR versus the NHIN. I'll just say NHIN for convenience, apologies, in that you may not have demonstrated the highest level of compliance to get access to the EHR, but if you connect from there through to the NHIN you have to meet that higher level of assurance just like you do for controlled substances. Is that the analogy that you were trying to make?

Deven McGraw – Center for Democracy & Technology – Director
Yes. And even though I think there might be a more clear policy justification on the DEA side because of their interest in cracking down on diversion and other criminal matters, if we think about the NHIN as wanting to establish a high best practices standard for the participants then it's a similar, although not equivalent justification. I actually do think you articulated it quite—

Paul Egerman – Software Entrepreneur
Deven, one question I had was who are the participants? Is it every user of an entity that participates?

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
If UPMC participates in the NHIN, then every EHR user at UPMC has to do two factor authentication?

Deven McGraw – Center for Democracy & Technology – Director

When they're connecting to the Nationwide Health Information Network.

Carl Dvorak – Epic Systems – EVP
Deven, I think there's a flaw in that thinking, though, in that a user won't really have knowledge of when and if they're connecting or subsequently causing the computer to connect to the NHIN to transact activity on their behalf. So for example if they order a lab test, the patient has to stop down to the lab to get a draw. That lab specimen may go out of the building to a third party referral lab to be processed, and a transaction may flow at the moment that specimen leaves the building, but not necessarily when the doctor's logged on. The doctor may have no awareness of whether that lab's processed in house or out of house. So I think the notion that you can track when a person is connecting to the NHIN is a flawed notion. If we don't deal with that up front I think we're going to have really confusing policy guidance later because it's not as directly apparent as one might think it sounds as we compare it to DEA controlled substance prescribing, for example.

Deven McGraw – Center for Democracy & Technology – Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think what we should assume is that the system will need to know when to ask for two factors. An individual person user should never have to know and decide, oh, I'm going to give two factors now. The system needs to detect that. Theoretically, the system would know when you're going across the NHIN or whatever. However, I would argue that a person never connects to the Nationwide Health Information Network. It's always a gateway for a …. It's not a person. It's an entity, to use our usual lingo, so they'd never connect.

Carl Dvorak – Epic Systems – EVP
But the person, I'll just get technical there, SAML assertion declares that the person that initiated this transaction has been assured at a certain level or not and the receiving entity could continue to reject that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think the discussion of SAML assertion is an entirely different discussion. I would hope so, at the very least.

Carl Dvorak – Epic Systems – EVP
I think the point I was trying to get at was that when you authenticate to a system and your system, at whatever level you authenticate at, information about how certain that system is about your identity can be passed on to another system, which could make a decision to say that's not good enough for me. I need additional credentials.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I would argue that that's a use case that this tiger team hasn't undertaken yet.

Carl Dvorak – Epic Systems – EVP
It's critical to this distinction that we're trying to make between accessing the EHR at one level and the NHIN at a different level.

Paul Egerman – Software Entrepreneur
Yes. I would frame the issue a little differently. The question is, is an EHR user the same as an NHIN user if the organization's participating in NHIN?

Deven McGraw – Center for Democracy & Technology – Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And I would say no, because the NHIN never sees a person user, whereas, an EHR does.

Paul Egerman – Software Entrepreneur
Yes, but if the answer's no then our recommendation has—you're saying they're not the same, but you're also saying that there is no such thing as an NHIN individual user.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right.

Paul Egerman – Software Entrepreneur
Then our recommendation doesn't make any sense, I think.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I don't understand that logic. If I'm sitting in front of the EHR and the patient says I have records at another hospital in another city where I was treated, the physician can make a decision to access those records. At that point he's a user of the NHIN. Now it's mediated through his computer, through his EHR, but his identity has to be passed on to the NHIN services and at that point that remote service could say, you haven't proved yourself sufficiently for me to grant you access. I need to know some more credentials or it would say you're fine.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I don't agree with that. I think that the NHIN connection itself, and I know we're technical here, but it's important, the NHIN connection itself is totally encrypted. The NHIN doesn't know the person whose information is going across that network. The EHR at the other end definitely has to authenticate that user, but not the NHIN itself.

Carl Dvorak – Epic Systems – EVP
Also, the transactions will likely be incurred, not necessarily by the physician, much of that will happen at the front desk, and especially after the initial connection. So if that patient is routinely moving back and forth between two sites, I don't think you want to encumber the physician with that, having to sign on to make that happen when in fact that information would generally be incurred to flow from a front desk registration process.

Paul Egerman – Software Entrepreneur
To take the argument one step further, Carl, the person at the front desk has access to the information.

Carl Dvorak – Epic Systems – EVP
Right.

Paul Egerman – Software Entrepreneur
And the person at the front desk has access to at least some of the information that's coming through from the NHIN, but does that make him an NHIN user?

Carl Dvorak – Epic Systems – EVP
Typically they won't necessarily have access to the medical information. They'll have awareness that the patient has data, they have a record elsewhere, and the desire to transport it. But although they may incur the transport of that record, they won't generally have access to the content of it. But it will arrive and the physician then will have access to the content of it when they see the patient in due course.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I need to bring up one tangent to this last discussion, which is I'm sure that many EHRs once somebody makes a request to the NHIN for information, that the data, even if it's retrieved upon a specific physician's request, once that physician receives that information, that EHR receives that information, that information will get integrated into the EHR. So even though the physician made the first request, that's only one person on the EHR side that's going to be potentially accessing that information, and it can be accessed by a dozen or many more people.

Deven McGraw – Center for Democracy & Technology – Director
Yes, well undoubtedly once it comes into the system it's subject to—

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
The authentication really only provides limited protection anyway.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm really uncomfortable with this whole notion that a user, a person user is going to make a request to the NHIN network. They never would make a request to the network itself. They would always pose a request to a Web application or to a gateway at the other end. It would never be the NHIN network itself. You'd never have a physician go out there and say, NHIN, get me Dixie Baker's record. That's just not the way it works.

Paul Egerman – Software Entrepreneur
Let me make a proposal as to how to see our way through all of this. A way to look at this is to say what we're going to be doing is rather than trying to change HIPAA relating to authentication and rather than dealing with EHR certification, we are going to deal with authentication from a standpoint of NHIN governance. As part of NHIN governance, or NW-HIN governance, we would say that an organization, an entity that chooses to participate in NW-HIN has to, at a minimum, have two factor authentication for any remote users of that EHR system.

Adam Greene – Office of Civil Rights – Senior HIT & Privacy Specialist
Paul, an additional issue here is I'm not sure that providers tend to actually participate in the NW-HIN themselves, NW-HIN or NHIN, whatever you want to call it. It's generally going to be the health information exchanges, except for some large integrated delivery systems, that are going to be participating.

Paul Egerman – Software Entrepreneur
I don't think that's correct.

Joy Pritts – ONC – Chief Privacy Officer
I don't think that's correct the way it's been described. It is intended to include the end users in some fashion, but you're right about the governance piece of it focusing, I think, on the intermediaries or the health information exchanges. So it's a fuzzy line there as to what the borders of this are.

Deven McGraw – Center for Democracy & Technology – Director
But I think what Paul's suggesting, and I'd like him to continue, is that the governance, even though the entities that may be governed may be the infrastructure entities, that will have to trickle down into sets of requirements for the participants.

Paul Egerman – Software Entrepreneur
That's right. We already have, for example, requirements that we put forward for certificates for the entities and so I'm saying as part of governance you would say is this for the entities that participate, they have to have a certain base level of authentication for their remote users. The argument being if they don't have this certain base level of authentication for the remote users some evil doer can sign on to one of the healthcare organizations remotely and gain access to some information in the national network. It's the weak link concept. My starting point is to say let's look at NHIN governance as our vehicle. Say we're going to use that to establish a baseline authentication rule for remote access to the EHR systems or entities that are participating in NHIN, so as a starting point see, does that framework work, and then we can discuss what the base authentication will be.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I really like that approach. I think that's exactly the right way to go. I would just ask you, when Dr. Blumenthal brought up the whole requirement of two factor for NHIN exchanges, he was talking about remote users logging into an application that was connected to the NHIN, is that right?

Paul Egerman – Software Entrepreneur
..., and the way I'm looking at it is if we frame it the way I'm framing it we can skip what they're logging into, for that matter. They're probably logging into their EHR system. I'm trying to skip that discussion.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I didn't mean to bring that part up. I meant if you're a user within a hospital that's connected to the NW-HIN, he's not saying that would require two factors, but if you're coming into that hospital remotely it would.

Paul Egerman – Software Entrepreneur
Right. I'm using that as a starting point. We could also talk about the internal users.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is such a slippery slope. It's hard to determine who's in and who's out.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I know. But I do like the approach, Paul.

Paul Egerman – Software Entrepreneur
I agree that's a slippery slope, David, but if you don't mind being on the slope for a few minutes, because we can then talk about whether or not we want to expand remote usage and how we define that. But right now I'm saying it's an issue of NW-HIN governance and if an organization is participating in NW-HIN then the remote users have to have a baseline authentication level.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Does "participate in the NW-HIN" mean that information can flow between—

Paul Egerman – Software Entrepreneur
It's one way or the other, yes, in or out information is flowing through.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So if you are connecting to a system which itself connects such that data can flow to the NW-HIN, then you must meet the level of certainty that the NW-HIN governance will set.

Paul Egerman – Software Entrepreneur
I really love working with technical people. You always bring up something. When I said "participate" I meant the organization was like, I don't know, UPMC, and UPMC participates in NW-HIN because they send laboratory results out, they send CCDs, whatever are going back and forth. And it's not the second order issue, it's just they're participating. If they're connecting through an HIE organization, then they're participating.

Deven McGraw – Center for Democracy & Technology – Director
Or they directly signed up to be part of the Nationwide Health Information Network. And they're not using an HIE, but they're directly connecting and they've ascribed to the standards and protocols of the Nationwide Health Information Network.

Paul Egerman – Software Entrepreneur
That's right, if they have the secret handshake, whatever the concept is. But if they're part of NW-HIN then NW-HIN governance applies to them. So if NW-HIN governance applies to them, part of NW-HIN governance would be that there would be a base level of authentication for any of the remote users.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Are we including what used to be called the NHIN Direct, it's now called the Direct Project, in our definition of NW-HIN?

Paul Egerman – Software Entrepreneur

I don't know.

Deven McGraw – Center for Democracy & Technology – Director
I think it depends on how the governance rule comes out. Recall that what's already been decided by the Policy Committee about governance is that it is voluntary. So whether ONC and CMS use their spending powers, and Direct I don't think involves grant programs, but there are other mechanisms that can be used to either encourage or require participation in the Nationwide Health Information Network. But it has always been described as voluntary but desirous of creating a trust framework that would promote trusted exchange among diverse participants using common standards protocols and best practices.

Joy Pritts – ONC – Chief Privacy Officer
Deven, it's also been stated that there is the desire to eliminate some of the distinction between directed exchange and what used to be known as the NHIN Exchange Project, because they are both seen as a means of exchanging health information nationwide. So I think that distinction will, at least as it's been articulated, will evaporate at some point.

Deven McGraw – Center for Democracy & Technology – Director
Right. I think that makes sense, because what we're talking about is governance of exchange, not mechanism of exchange. We want everybody to ideally be governed by a common set of rules and policies, but whether they're doing so directly or they're doing so through an HIE should not matter.

Joy Pritts – ONC – Chief Privacy Officer
Right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So it seems to me that the points Carl has made are important, which is that much of this information flow across these systems for someone who's participating, be it direct or be it NW-HIN, much of that information flow is automatic and triggered by processes of care and workflow. So I think the implication would be that a user might be logging into his EHR and seeing data that has been pulled down or pulled across regardless of whether he pushed a button and said "Do it" or not.

Deven McGraw – Center for Democracy & Technology – Director
That's right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
To me that's kind of transitive property says therefore that person logging into the EHR has to meet the same level of assurance that would be set by the NHIN governance.

Paul Egerman – Software Entrepreneur
That's correct. In other words, I'm just saying that NW-HIN governance would establish a base level alerting you to the recommendations of what that base level is, the base level, and that is going to apply to all remote users in the EHR.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That sort of implies to me that Dr. Blumenthal's notion of calling out NW-HIN access for special treatment doesn't make sense anymore, because we're saying that any of the data in the EHR could have come from NW-HIN Direct.

Paul Egerman – Software Entrepreneur
It only makes sense to the extent that not every healthcare organization necessarily participates in the NW-HIN.

Deven McGraw – Center for Democracy & Technology – Director
That's right. ... NW-HIN as a policy vehicle—

David McCallie – Cerner Corporation – Vice President of Medical Informatics

But if we sweep Direct into this, then I think it will effectively be almost every physician.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
By design, that's what Direct was trying to do.

Deven McGraw – Center for Democracy & Technology – Director
Right. I think it just sort of depends. Direct was intended to provide a mechanism for exchange that didn't necessarily require you to have a connection to an HIE, to be able to send directly through secure message from one to another, right? So it's about a mechanism of exchange, and to the extent that there's governance tied to that it's voluntarily adopting the standards so that there's interoperability, right?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But Joy was trying to say we're going to try to erase the distinction between the risks associated with what I would call direct versus indirect or sharable—

Joy Pritts – ONC – Chief Privacy Officer
No, what I'm really trying to say is that the Direct Project was a pilot and an entity can do directed exchange and do exchange through an HIE, right?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I thought you were saying that we should treat those the same from—

Joy Pritts – ONC – Chief Privacy Officer
They're all going to be considered in NW-HIN. Now, I believe from the way the governance has been approached to this date, was that there are potentially going to be distinctions based on different functionalities, right?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right. That was the whole goal of creating Direct, was to create a lower risk profile because it was point to point.

Paul Egerman – Software Entrepreneur
Are you asking, David, that whatever the authentication concept is that there be a carve-out for NW-HIN Direct, or for some—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
No. Actually, I think our whole work has treated Direct as somewhat of a carve-out because of the difference in consent policies that we articulated in one of our earlier report outs. So we have chosen to create a distinction. I was a little surprised to hear what I think I misinterpreted Joy to say, that we wanted to erase those distinctions.

Paul Egerman – Software Entrepreneur
What I'd like to do is—

Joy Pritts – ONC – Chief Privacy Officer
What we want to eliminate is NHIN Direct distinctly from NHIN Connect.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Although we have carved out special consent differences already.

Joy Pritts – ONC – Chief Privacy Officer
Based on functionality, but when we use the term "NHIN" we expect there to be multiple modes of participating.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So now we just can't use the word "NHIN" to distinguish between them—

Joy Pritts – ONC – Chief Privacy Officer
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But we now have to talk about the mode, so we're right back where we started from.

Joy Pritts – ONC – Chief Privacy Officer
Well, yes and no.

Deven McGraw – Center for Democracy & Technology – Director
I think you can say that there could be some policy that would vary by mode of transport but not all would need to vary. We have some very specific reasons that we laid out for asking for consent in certain exchange models that were very clearly articulated in those recommendations. Here, I'm not sure it makes sense to draw that distinction, although we are, at least in the recommendation that's currently on the table, trying to see if there is a distinction worth making between access that is remote versus access that is internal.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
One footnote is I understand that we may treat consent differently than level of assurance.

Deven McGraw – Center for Democracy & Technology – Director
That's right.

Paul Egerman – Software Entrepreneur
I'm confused on this discussion, David. Are you okay with the proposal I'm saying, that this is an NW-HIN governance issue, or are you asking for a carve-out for NHIN Direct?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
No. I didn't raise the NHIN Direct yet because I wasn't sure that we had grappled with the other case. So I wasn't really ready to even raise that question in my own thinking. But my point is back earlier, which is the connectivity of these systems and the seamlessness with which the data needs to flow for workflow purposes. To me implies that it will be very difficult, either you're connected or you're not connected, but once you're connected then pretty much all the data exposed to someone who has access to EHR could have been fetched.

Paul Egerman – Software Entrepreneur
I agree. So that's why I'm saying that if an organization participates in NW-HIN, then they have to have some base level of authentication for their users.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I agree. Then that led to the question of what does "participate in the NW-HIN" mean?

Paul Egerman – Software Entrepreneur
Okay. What I'll do is I'll let the attorneys figure that one out.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Paul Egerman – Software Entrepreneur
Okay? So let's go back to basics. Are we in agreement that if you participate in NW-HIN there needs to be some base level authentication rules, in terms of NW-HIN governance? Do we have agreement on that concept?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Deven McGraw – Center for Democracy & Technology – Director
Yes.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

W
... there.

Paul Egerman – Software Entrepreneur
So to limit the discussion a little bit, let's first look at remote access, which I'm going to define as access to the EHR over the Internet.

Deven McGraw – Center for Democracy & Technology – Director
Or an unsecure connection?

Paul Egerman – Software Entrepreneur
No, over the Internet, a public network, the Internet. So my question is, if you're a user of an EHR system that is connecting over the public network, the Internet, what is the base level that we are going to say? Is it two factor? Is it NIST Level 3? Is it something else?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Level 3, I'll open the discussion.

Paul Egerman – Software Entrepreneur
One vote for Level 3. It's not surprising the security guru says Level 3.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think there are two things that go into my saying that. Number one is that, and probably number one and number two, there's already a standard in place so we're not making it more complex than it needs to be.

Paul Egerman – Software Entrepreneur
Okay. Any other views?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
As you know, I'm worried about the definition of "remote," but let's just leave that off for a second and I will allow that maybe we can define what remote means. I think there's a middle ground between single factor, password only versus NIST Level 3. And unfortunately we don't have a name for it, and internally here we sometimes refer to it as one and a half factors.

Paul Egerman – Software Entrepreneur
So you've got to basically vote for more than one, a two factor approach, but that is not as strict as Level 3.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Correct. More than one, but it may not meet the rigid standard of NIST Level 3.

Paul Egerman – Software Entrepreneur
I'm just curious to know, those are two approaches on the table, is there anything else?

Carl Dvorak – Epic Systems – EVP

I would add the comment that I think to go to Level 3 would adversely affect usability for clinicians without necessarily reducing the risks that are aspired to. So I would think Level 2, with maybe some additional precautions and requirements, and not to go to Level 3 until we really study it in depth and understand if we really truly are mitigating the risks better, and discussed when we discussed about Level 3.

Paul Egerman – Software Entrepreneur
Would it be fair to say we have two concepts on the table? One is Level 3 and the other one is—

Deven McGraw – Center for Democracy & Technology – Director
Greater than Level 2.

Paul Egerman – Software Entrepreneur
Yes, greater than Level 2. At least two factors but somehow maybe the Standards Committee or somebody defines what the two factors are.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie. I'd like to put the third as, which I also could live with, is the same as DEA. I would like for us to avoid having to come up with our own flavor of two and a half. The DEA already has come up with a two and a half, so I would suggest that would be—well, plus, if you think about certifying products, we don't want to require that products not only be able to support the DEA two factor for controlled substances. But this other flavor of two and a half, I think it gets too complex.

Paul Egerman – Software Entrepreneur
Dixie, would it be okay, though, if I just merged that with the Level 3? In other words –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
No, because it is softer, because—

(Parties speaking simultaneously)

David McCallie – Cerner Corporation – Vice President of Medical Informatics
... in Level 3.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
They allow biometrics and Level 3 does not.

Paul Egerman – Software Entrepreneur
Okay, so there are three things on the table. There's Level 3, Level 3/DEA, and—

Deven McGraw – Center for Democracy & Technology – Director
And two factors.

Paul Egerman – Software Entrepreneur
And two factors defined by the Standards Committee.

Deven McGraw – Center for Democracy & Technology – Director
Yes, and I think bringing Carol's point back on to the table, I think it's really important to build the evidence base on what's effective here. I think part of the reluctance of some to go as high as a hard requirement for either DEA or NIST Level 3 is that, again, in both of those cases there were countervailing considerations that drove them to the stronger level: law enforcement in the DEA case, and got access to government protected data in the case of NIST. It's a government framework, and I think that we heard a lot of noise that we haven't dug into and we probably wouldn't be able to dig into in any timely way about what really works here. Nor do we necessarily know how well the DEA rule is going to work because it's effective very recently and entities are just now grappling with having to put it into place.

Paul Egerman – Software Entrepreneur

Deven, you're making an argument for, I'm calling it option three, some two factor defined by Standards Committee.

Deven McGraw – Center for Democracy & Technology – Director
I am. And it's not as strong, but I want to couple that with a strong recommendation to study the implementation of the DEA rule because I want to migrate to something more strong and certain, but it just feels premature.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I don't have it in front of me and I don't remember enough, but we had some really great testimony at one of the Standards Committee meetings about a year ago from privacy and security people from outside of healthcare. I remember Peter Tippett from Verizon, I believe, and some others who gave some pretty strong and interesting data about what works and what doesn't work in, for example, the banking industry. So it has been very well studied in other areas, not necessarily in healthcare, but I don't think we're completely as ignorant about the tradeoffs in the broad technology world as we are may be in healthcare. But that notwithstanding, I do agree with Deven. I think that we aren't yet sure what the impact on workflow for the DEA standard, which is itself a mitigated form of Level 3 is, and people are worried about it. It took years to get that standard hammered out because there was so much concern, and it would be probably ill advised to set such a high bar that we preclude people even trying to use these systems.

Carl Dvorak – Epic Systems – EVP
I'll add one more thing. I believe that this work should be strongly use case driven. I think the notion that we can apply policy decisions without fully understanding the use case will likely lead us into a contorted implementation of NW-HIN over time. So I'd like to make sure that as we think about progressing that we take an appropriate pause and define the use cases and how this information really will flow, and then make sure we apply the right and reasonable levels of security and assurance to that.

Paul Egerman – Software Entrepreneur
So a question I have is, I don't know whether or not we have a consensus around this, because I hear Dixie advocating for either Level 3 or Level 3/DEA. My question is, first of all, do other people agree with Dixie's view? Secondly, Dixie, could you live with this alternative, or do you firmly believe it should be Level 3 or Level 3/DEA? Let me ask first, besides Dixie is there somebody else who would like to speak to doing the one on the first ... Level 3 or Level 3/DEA?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I'm firmly in Carl Dvorak's camp.

Deven McGraw – Center for Democracy & Technology – Director
Leslie Harris had to drop off the line early, but I recall from an earlier call that she was aligned with Dixie on this.

Paul Egerman – Software Entrepreneur
Leslie Harris or Leslie Francis?

Deven McGraw – Center for Democracy & Technology – Director
I'm sorry. Leslie Harris had CDT. I meant Leslie Francis.

Paul Egerman – Software Entrepreneur
Yes, because otherwise, you get two votes and that's not fair.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I don't know what the right answer is here, but I will say that David McCallie reminded me that in the testimony that we heard from other sectors, and David, correct me if my recollection is wrong, because you're right it was about a year ago, but we did here that Level 3 is certainly being implemented in other sectors.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
We did, although the PCI standard, the one that the credit card industry uses, is certainly not Level 3. It's that one and a half.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
No, no. Yes, yes, yes, that's clearly not.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I got an impression from Tippett's testimony, at least what sticks out in my memory was that that's not the weak link and that if you're worried about that you're probably going to miss something really much more profound, which is you have to take a system-wide view of the risks.

Paul Egerman – Software Entrepreneur
So, could we do it this way? Could we say that we have a consensus that for NW-HIN governance; that it needs to be established a base level of EHR authentication, which needs to be at least a two factor authentication level? Some people want to go further and do NIST Level 3, but it needs to be at least two factors and report that to the Policy Committee. Also suggest, as Carol said, there needs to be research and also suggest that the Standards Committee has got to figure this thing out.

Deven McGraw – Center for Democracy & Technology – Director
Here's another additive to this suggestion. I'm ready to be as done with that authentication topic as anyone else, but another option, because authentication sits within a constellation of other security protections, is that we consider this consensus that we've roughly achieved. And move on to both the patient piece but also some other security issues, so that we can think of security for information exchange more holistically and make sure all the pieces fit together?

Paul Egerman – Software Entrepreneur
Except that we want to report ....

Deven McGraw – Center for Democracy & Technology – Director
Yes. We would report that, but again I think it's still worth continuing to think about this as just one element of an overall security program, as opposed to not taking it into context. That's all. Again, I wouldn't hesitate not to report on it to the Policy Committee, but to note that we've got to flesh these other pieces out. It might actually be helpful to us either in reinforcing the decisions that we're making in authentication or if at that time we feel like we need to do something more on authentication because other elements are weaker, which I doubt is going to happen, then we would do that. I think, quite frankly, that we'll feel better about this if we strengthen the other components of security.

Paul Egerman – Software Entrepreneur
Maybe that's right. We also might feel better once we've come up with an approach for patient access and when we look at it holistically, this is what the patient's doing or this is what the EHR users do.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I want to make two more points. Number one, I'm all for research, I always am for research, but there's been a lot of work done on user authentication, so I think when we talk about research we should be looking at the body of work that already exists, more than going out and reinventing the wheel. The second point is I think we need to also consider what the federal partners will require of a private user that may want to access their systems. For example, if a physician wants to get a record from the VA or CMS or the military health system, are they going to require another level of authentication? I think our solution needs to think about this holistically and not just the private sector on the NW-HIN.

Paul Egerman – Software Entrepreneur
Excellent comment.

Deven McGraw – Center for Democracy & Technology – Director
Yes, and it almost reinforces Carl's point about certain use cases—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Deven McGraw – Center for Democracy & Technology – Director
—... required.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think it's risk-based. Use case is one way to segregate risk, but it's really to take a risk-based analysis, and the risks differ.

Paul Egerman – Software Entrepreneur
Okay, have we reached a conclusion on this? Are we able to go on to patient access?

Deven McGraw – Center for Democracy & Technology – Director
I think the one other dangling issue is the one about the distinction between remote and internal and whether we try to mine that a little bit more or allow Standards to help us out.

Paul Egerman – Software Entrepreneur
Here's what I propose to do, to define remote is not remote access, but access over the public network, which means the Internet.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That's even an odd definition these days, because I know a lot of carriers route small practices over public networks, but with appropriate VPN concentrators and such. So we'd probably have to dig into that definition. I'm sure that's going to be called into question along the way.

Paul Egerman – Software Entrepreneur
I'd have to say a VPN over the public network is still over the public network. So I would count that in my definition of remote access. In other words, there's something going on when you do that VPN and so whatever process you need to do to create it probably counts as part of your authentication process. But still—

David McCallie – Cerner Corporation – Vice President of Medical Informatics
The key notion of what remoteness means is that you're not under the scrutiny of something local that could determine that you're not supposed to be doing what you're doing. If you walk into a small physician's office and you're the sole proprietor of that office and you sit down and VPN into something, I don't think that's actually remote, because you're in the place that you're supposed to be and there's people looking at you and saying, yes, he's supposed to sit there and access this computer. We have remote hosted EHRs at 300 or 400 hospitals and they all go over the network, but they're not remote. That's why I earlier registered my concern that "over the Internet" isn't a sufficient definition. It's really almost the point of origin where there's a security ever present at the point of origin of the access.

Paul Egerman – Software Entrepreneur
An easier way to do it might be to drop the concept of remote access and just say it's all EHR users.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think that's where you end up.

Paul Egerman – Software Entrepreneur
So then our comment is at least two factor authentication for all EHR users.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
With taking into account the use case or the risks, depending upon—

Paul Egerman – Software Entrepreneur

That's right. If the Standards Committee decides this is going to be NIST Level 3, if you have a situation like I think of some vendors, a direct connection between the terminals in the healthcare organization and in the computer that's located in the healthcare organization, whether or not you consider physical security data to enter the facility one of the factors. So it goes back to what Carl said, you've got to look at some of the use cases to figure it out.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
And Dixie join in here as well, I'm not sure the Standards Committee is going to be able to get too far away from some of these policy decisions. Because it's pretty easy to enumerate what the candidate factors are, but it then comes back to policy as to which ones are required, because there's a tradeoff of complexity and cost and workflow interruption that isn't a technical issue anymore, it's a policy issue. So don't expect too much from the Standards Committee.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's a very good point. You'll likely get it batted right back at you.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, because that's what we did in Direct, every one of our conversations we came down to that's a policy question.

Deven McGraw – Center for Democracy & Technology – Director
Right. That's fair. I think we just need to acknowledge that there are some circumstances under which we would want to, on a circumstances, risk use case basis go back and revisit the policy on that. Just to give an example, is to say when we get to the policy questions that surround query response models involving the ability to query a patient index, for example, would we vary the authentication required to do that? Maybe we would and maybe we wouldn't, but that presents a particular set of circumstances under which to judge whether the baseline that we've set today is sufficient.

Similarly, there are distinctions with more sensitive data under state law that might have some additional requirements attached to it that if that were squarely presented as a need of policy guidance, we would have something more concrete to deal with. It becomes very hard to speculate on what that might look like absent a particular set of issues that are in front of you. So I think we could, as a general matter, say what we want to say but talk about the consensus that we've just achieved, but acknowledge that it is always a balance of risks. That it often depends on the other security mechanisms that are in place and we may need to revisit it for certain particular use cases or circumstances. Does that make sense?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
It sounds good to me.

Deven McGraw – Center for Democracy & Technology – Director
Because we don't have a capacity to judge what those risks are absent a particular set of circumstances in front of us.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is making them addressable, right?

Deven McGraw – Center for Democracy & Technology – Director
In many ways. In some respects, yes. I'd have to think more about whether that analogy is exactly right. But it's setting out a setup of general requirements or recommendations but specifically acknowledging that particular circumstances may require more. It's not meant to be the be-all and end-all of what we might say on this issue going forward forever.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Is it consistent to say that the floor is higher than a single factor? In other words, the floor is higher than a password?

Deven McGraw – Center for Democracy & Technology – Director
Yes.

Paul Egerman – Software Entrepreneur
Yes, this is at least some sort of two or more factor.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Okay, some additional factor. You have to be careful when you say "two factor" because if that is coupled to the rest of the sentence in the NIST document, one of which must be something you know, one of which must be—

Paul Egerman – Software Entrepreneur
Yes, that's right. But we're not saying that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
We're not saying that. We need to be precise, that it's additional parameters, other than a password, to be determined based on the risk.

Paul Egerman – Software Entrepreneur
We will write this up, and we will need to do some careful wordsmithing to make sure it's correct, and so we'll have to run it by everybody.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think another factor to consider with respect to VPNs, and I'm agreement with what David said about VPNs, they are all over the place, but VPNs are also used to transact and store things and access things in the cloud routinely, and I know that routinely they are treated as if they're a private network.

Paul Egerman – Software Entrepreneur
It sounds great. So we have this brief moment of equanimity. I'd say we've got this issue solved. What do you want to do, Deven? Do you want to spend 15, 20 minutes to launch into the user patient access side?

Deven McGraw – Center for Democracy & Technology – Director
Yes, I think so. Because we're always better trying to wordsmith stuff off line and get it out to folks. We actually have two other calls before the April Policy Committee meeting. We did these slides before the meetings for the tiger team were scheduled for the month of April, we actually have the meeting on the 23rd and also one on April 6th before the next Policy Committee meeting, which is April 13th, I think. At any rate, we'll have some time to make sure we got this right whether we wordsmith off line, which is always highly desirable, or online. But my sense would be that we can at least do some of the background that MITRE helped us prepare on the patient identification and authentication issues, and so we'll get the baseline stuff out on this call and then really begin the discussion in earnest on our next call. Does that make sense?

Paul Egerman – Software Entrepreneur
Yes.

Deven McGraw – Center for Democracy & Technology – Director
Okay. So do we still have Renee from MITRE on the line?

Renee – MITRE Corporation
Yes, I'm here. Go to slide 12, I believe?

Deven McGraw – Center for Democracy & Technology – Director
Yes. There you go.

Renee – MITRE Corporation

I'm just going to set the scope of the discussion first. Part of the required core measures for the eligible provider and hospitals for stage one of meaningful use is to provide the patient with an electronic copy of their health information upon request. So as more and more patients are possibly accessing their record via a Web portal, this is going to require a need to establish and validate the patient's identity prior to access. So just to sum that up, the scope of this discussion is limited to the identity proofing and authentication of patients.

But who is the patient? So this is just important to define who we are talking about. First, the patient, the person actually receiving those healthcare services and who would like to access their information, but there's also the consideration of a proxy to consider. A proxy is a person that might be making medical decisions on behalf of a person, such as the parent of a minor, next of kin, a spouse, etc. So it's important to ... we're not only talking about a patient but we could also be considering a healthcare proxy.

Carl Dvorak – Epic Systems – EVP
Can we interrupt here or not?

Renee – MITRE Corporation
Sure.

Carl Dvorak – Epic Systems – EVP
I was particularly concerned with the phrasing on that second bullet point where it says "on behalf of person who is unable to do so," we see a tremendous number of proxy users and it's not that the person is unable to do so, it's that the person appreciates the help. Generally, it happens in the senior category, where the senior is still allowed to make their own medical decisions but they appreciate the help and assistance of a son or daughter, who may live in a different part of the country. So I was going to suggest you want to be really careful with the "unable to do so" language, because that might imply something stricter than we see people making use of in practice.

Renee – MITRE Corporation
That sounds good. Thank you for that comment, Carl, good point.

Deven McGraw – Center for Democracy & Technology – Director
Good point, Carl.

Renee – MITRE Corporation
We can go on to the next slide, number 14. So now that we've talked about who we're talking about bringing up particular scenarios. So this will be a patient or a proxy that might be accessing the healthcare information patient portal, such as requesting a renewal of a prescription, such as the VA's Blue button, where they're actually viewing or printing off parts of the record, also maybe receiving or sending secure messaging, or even accessing a personal health record.

Before we get into some of the questions that we might have keyed up here for the tiger team, it's important to distinguish. Since we were just coming from user authentication and we're switching over to patient authentication, for the user authentication part we had already assumed that they've already gone through some form of identity proofing with their particular organization. But when we're talking about patients, we need to consider both identity proofing and authentication. So just an important distinction that the slide is here to prove .... We're also considering identity proofing of the patients. So just turning it back over, I believe, to Deven and start the questions.

Deven McGraw – Center for Democracy & Technology – Director
No, you got it. We asked for MITRE to help us scope out some potential questions here. I think it probably makes sense in the limited amount of time that we have here to just quickly go through these. Then get your feedback on whether or not this is the right set of questions, whether we've left something out, whether there is something else we need to explore, and maybe given the issues around proxy access, that we want to consider that too, maybe we should start calling this patient and proxy access.

That's really optional. But I found that to be a really helpful part of the conversation. It's not always just the individual, himself or herself, who's going to be accessing the information.

Identity proofing, this is really about verifying the identity of the patient and/or the proxy, who should really perform identity proofing, what method is used, or what method is acceptable to be used in identity proofing, what is the acceptable documentation of identification, and should the documentation be required to be verified. Then on the authentication side, this is obviously proving is this patient or the proxy who he or she says he or she is, what's an acceptable method of authentication, so we're back in somewhat similar set, if not the same set of issues that we just spent some time discussing on the provider side.

I want to stop here and see, again, is this the right set of questions? Are there other questions that should be on this list? Are there any that should be removed? Does anybody want to provide some suggestions for how we attack this set of issues effectively going forward?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Having gone through a bunch of this type of stuff, there really is a third use case that is different that you might say is similar. We have a case where we actually take and export patient information to a third party PHR and there's a lot of considerations around setting up that initial match and initial authentication in order to set up the pairing with the PHR. I think what you're going to find is that that is going to be a way that a lot of people are going to want to access information, is they're going to have to establish a PHR. They're going to want to have that information linked, and how do you identity proof, authenticate, set up the pairing so that that occurs.

Deven McGraw – Center for Democracy & Technology – Director
So are you suggesting that that might have a different set of policies or recommendations than those for an internal portal?

Paul Egerman – Software Entrepreneur
I think that the use case that you're describing, John, is interesting, but it's really not the same challenge. Even though the previous slides mention PHR, I would suggest that an easier way for us to get our work started is to think about the patient portal, which is a likely component for meaningful use stage two. So the way I'm thinking about this is if there's going to be possibly a patient portal in meaningful use stage two, what is the patient authentication process to view that portal, which is not the same as the PHR. You're actually looking at, in effect, a view of the patient's record in the EHR system.

Joy Pritts – ONC – Chief Privacy Officer
John, can I ask you a question? You raised a specific use case; do the questions that are posed address part of your use case and then you layer that last level on top? Or is it a totally different use case?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I think it layers on top. Let me say that we have a PHR internal to our organization that is actually part of an EHR, but we also have consumers that want us to, in essence, export information to a PHR. Not just export once, but keep a persistent relationship in place such that if there is new information that it also gets exported to that third party PHR. So there's actually a little bit more work that needs to be done to ensure that yes, the patient is who they say they are, so if we start an export that we know it's them that's actually asking. Then we need to know, from the PHR vendor perspective, where we should be shipping information, making sure that it's correct, make sure that that persistent relationship stays in place and is appropriate. And so in some cases it's really a matter of making sure that that persistent relationship needs to continue. It's just that we have both of these types of situations occurring today.

Paul Egerman – Software Entrepreneur
Those are good comments, John. I just view that as, additional use case, you called it, Joy called it layering, a layer above where we are in this discussion. We're talking about really patient authentication. It's a consumer or a patient being able to, in effect, sit at their home on a computer or a laptop and

access their own record, which is a patient portal. Some people call it a tethered PHR, but I try to get away from the expression PHR, that this is a portal in the EHR system with information for that patient.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Right. All I was trying to add was the fact that we're already seeing use cases where people want the portal but they also want something else.

Paul Egerman – Software Entrepreneur
They want something else, right. This is step one of the portal.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think that Direct is going to facilitate this dramatically. We're seeing lots of PHR vendors implement Direct links to make this exact scenario happen, so it's going to grow.

Joy Pritts – ONC – Chief Privacy Officer
David, so your last statement there is in support of John's, that it's an issue you think that needs to be addressed sooner rather than later.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, but I agree with your supposition that we have to start with these same questions that are on the slide right now and then it's another step beyond that.

Joy Pritts – ONC – Chief Privacy Officer
Is that true also for the proxy, that you start with these questions and then the next step is you address these issues for the individual and then you address these issues as a next step for proxy? I think it's difficult to address them together. They present slightly different issues. Is that right, Paul? I think you were the one who was raising this.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
This is David. Just my two bits on it is, yes, I think that establishing the patient is step one. Then if someone asserts they have the right to be proxied, then that's another process that has to be accounted for.

Paul Egerman – Software Entrepreneur
That's right.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
That would validate that that's a—

Paul Egerman – Software Entrepreneur
Yes, you need some process by which the patient validates that this is their proxy.

Carl Dvorak – Epic Systems – EVP
... has to become proxy too. One obvious one that we think of is for an incapacitated adult or a minor child, but then I think we have voluntary proxies where a patient may just wish to give a loved one access to the chart. And I think we want to be careful not to encumber that second use case.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But if I show up and say that I'm Charlie Sheen's proxy, somebody ought to challenge that.

Carl Dvorak – Epic Systems – EVP
Absolutely, yes. If you claim proxy, that's one case. If the patient seeks to independently grant proxy, ultimately the patient can rent a billboard and put their medical chart up there if they'd like to. So I think we want to be careful not to prevent the case where a patient may want to grant it permanently or temporarily to another person.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
We've gone through all these proxy issues, both with adult and pediatric incapacitated, versus individuals who have the capacity to make decisions, and a proxy is very complex.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
It is.

Deven McGraw – Center for Democracy & Technology – Director
And keeping in mind, we don't have to write the laws on proxy.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Everybody's going to look to us, though.

Deven McGraw – Center for Democracy & Technology – Director
Yes, well it is a complicated set of laws that may differ in some respects from state to state, particularly where you're talking about more mature minors. So instead I think we will be very wise to just think about what are the policy steps that need to be taken assuming the need to comply with whatever is your combination of federal and state laws that apply for proxy circumstances, and not to try to rewrite those.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I just know that when we got into this topic we drove down into the weeds so fast because the weeds, unfortunately, really define how you solve the problem. So I think we're going to be really tasked ultimately to address some fairly heavy issues with regard to things like pediatric proxy, and we're not going to have a choice but to because without those details what we recommend is not going to be of practical value to most people.

Deven McGraw – Center for Democracy & Technology – Director
All right, point taken, but just be warned that it will be. I'm going to ask Paul and Joy to join me in this. I think it will be a challenge but we will, I think, have to try very hard not to get into the issue of who is an appropriate proxy and the circumstances under which a proxy can be granted and instead deal with the policy issues that surround when you have an appropriate proxy how do you honor that.

Joy Pritts – ONC – Chief Privacy Officer
Yes.

Paul Egerman – Software Entrepreneur
Yes. That's right. If we keep our focus very narrow and we say this is really about authentication and identity proofing, and we're going to not deal with how you decide who's an appropriate person to be a proxy and not deal with the pediatric issues of just who is a guardian and who is a parent. Those are interesting issues, but we're not going to deal with that. We're going to say, somebody else has dealt with that and has made the determination that an individual is a proxy, then you still have this business of identity proofing and authentication for that individual. So if we just focus on just those concepts I think we'll be fine.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I just think people will be asking for the other part very quickly, and I'm just—

Deven McGraw – Center for Democracy & Technology – Director
I suspect they will, too, but we don't even have the authority to set that. We can only do so much, John.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
I know. Having just been through all of this I just know where it's going and I just want to make—

Deven McGraw – Center for Democracy & Technology – Director
Everybody wants one clear answer.

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security
Yes.

Deven McGraw – Center for Democracy & Technology – Director
Yes. Okay, so it looks like we have the right set of questions to begin this discussion on our next call. It also looks like we have some different use cases that we might want to layer on top of this core set of questions, but we have some marching orders for moving forward. Paul, do you have anything else to add? I think this might—

Paul Egerman – Software Entrepreneur
No, I think we've made excellent progress today. We've advanced our view of the EHR user. We started to consider the issues associated with patient access, and again the main concept I want, as people think about us going forward, is if we look at patient access and we look at the patient portal and focus on the patient portal as our starting point, I think we can make a lot of progress. But that's hopefully what we'll be doing on the next call.

Deven McGraw – Center for Democracy & Technology – Director
Okay. Judy, do you want to open it up to public comment?

Judy Sparrow – Office of the National Coordinator – Executive Director
Yes. Operator, can you see if anybody from the public wishes to make a comment?

Operator
We do not have any comments at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. Thank you, Deven and Paul.

Deven McGraw – Center for Democracy & Technology – Director
Thanks, everybody.

Paul Egerman – Software Entrepreneur
Thank you, Judy, and thanks to Lisa and Joy also. Great call.

Public Comment Received During the Meeting

1. What part of Identity Assurance are you trying to mandate... provisioning at high assurance, or session authentication at high assurance? http://healthcaresecprivacy.blogspot.com/2011/03/authentication-and-level-of-assurance.html

2. "Remote access" is a red herring for the stated purpose of ensuring that user authentication meets a given security level for any user of an EHR system that connects to the NwHIN (i.e., permits/facilitates inquiries for data from other EHR systems). What you might want to recommend as a matter of NwHIN governance is that the Standards Committee recommend the "Best Practice" for use authentication in an NwHIN-connected EHR system, based on (1) re-enforcing patient trust in health information exchange, (2) commonly available / rapidly implementable technology and (3) giving due consideration to work-flow impact.

3. NwHIN (both direct and exchange) will often times be accessed by an automated task based on 'events' (e.g. schedule look ahead, summary published, results available)... so it would typically be done by an automation... BUT some accesses will be directly relatable to a user, related by way of cause-and-effect.

4. LoA can drive high Expense, (not just $$)... The expense demanded must be justified by the protection that it brings to THE RISK.

5. Note you don't need to force a LoA, as long as the protocols used communicate THE LoA of each identity asserted, the service side can enforce the LoA that THEY need to enforce http://healthcaresecprivacy.blogspot.com/2011/03/authentication-and-level-of-assurance.html

6. The discussion around which NIST assurance level to adopt for access to an EHR seems to be driven by whether the various authentication technologies consistent with Level 3 will be usable. I'd propose that Level 3 ought to be required because of the sensitivity of the kind of information that is being accessed, which is a patient's medical record. The criteria that ought to drive the decision about the appropriate level of assurance is the risk of harm to the patient (and healthcare provider) if the patient's medical information is compromised. That is, in fact, how these levels of assurance are defined….by the likely consequences of an authentication error. Although the current 1.0.2 version of NIST 800-63 is somewhat rigid about the kinds of authentication tokens required for Level 3, the NIST 800-63 draft of 2008 seems to allow for more flexible combinations of authentication technologies to meet Level 3. There was also a fear that adopting Level 3 will require EHR users to have multiple tokens to ac

7. No, NIST level 3 allows the possibility for a biometric to unlock the token, but doesn't require the biometric